

A class of three-weight and five-weight linear codes

Fei Li¹, Qiuyan Wang^{*,2,3}, Dongdai Lin²

Received: date / Accepted: date

Abstract Recently, linear codes with few weights have been widely studied, since they have applications in data storage systems, communication systems and consumer electronics. In this paper, we present a class of three-weight and five-weight linear codes over \mathbb{F}_p , where p is an odd prime and \mathbb{F}_p denotes a finite field with p elements. The weight distributions of the linear codes constructed in this paper are also settled. Moreover, the linear codes illustrated in the paper may have applications in secret sharing schemes.

Keywords Linear code · Weight distribution · Gaussian sums · Weight enumerator · Secret sharing.

Mathematics Subject Classification (2010) 94B05, 94B60

This research is supported by a National Key Basic Research Project of China (2011CB302400), National Science Foundation of China (61379139) and the “Strategic Priority Research Program” of the Chinese Academy of Sciences, Grant No. XDA06010701 and Foundation of NSSFC(No.13CTJ006).

F. Li

1. School of Statistics and Applied Mathematics, Anhui University of Finance and Economics, Bengbu City, Anhui Province, 233030, China

E-mail: cczxf@163.com

Q. Wang,

2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100195, China

3. University of Chinese Academy of Sciences, Beijing 100049, China

E-mail: wangqiuyan@iie.ac.cn

D. Lin

2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100195, China

E-mail: ddlin@iie.ac.cn

1 Introduction and main results

Let $q = p^m$ for an odd prime p and a positive integer $m > 2$. Denote $\mathbb{F}_q = \mathbb{F}_{p^m}$ the finite field with p^m elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ the multiplicative group of \mathbb{F}_q .

An (n, M) code \mathcal{C} over \mathbb{F}_p is a subset of \mathbb{F}_p^n of size M . Among all kinds of codes, linear codes are studied the most, since they are easier to describe, encode and decode than nonlinear codes.

A $[n, k, d]$ code \mathcal{C} is called linear code over \mathbb{F}_p if it is a k -dimensional subspace of \mathbb{F}_p^n with minimum (Hamming) distance d . Usually, the vectors in \mathcal{C} are called *codewords*. The (Hamming) *weight* $\text{wt}(\mathbf{c})$ of a codeword $\mathbf{c} \in \mathcal{C}$ is the number of nonzero coordinates in \mathbf{c} . The *weight enumerator* of \mathcal{C} is a polynomial defined by

$$1 + A_1x + A_2x^2 + \cdots + A_nx^n,$$

where A_i denotes the number of codewords of weight i in \mathcal{C} . The *weight distribution* (A_0, A_1, \dots, A_n) of \mathcal{C} is of interest in coding theory and a lot of researchers are devoted to determining the weight distribution of specific codes. A code \mathcal{C} is called a *t-weight code* if $|\{i : A_i \neq 0, 1 \leq i \leq n\}| = t$. For the past decade years, a lot of codes with few weights are constructed [3, 7, 9, 10]. Furthermore, there is much literature on the weight distribution of some special linear codes [1, 3, 5, 7, 13, 14, 21, 22].

Let $D = \{d_1, d_2, \dots, d_n\} \subseteq \mathbb{F}_q$. A linear code \mathcal{C}_D of length n over \mathbb{F}_p is defined by

$$\mathcal{C}_D = \{(\text{Tr}(xd_1), \text{Tr}(xd_2), \dots, \text{Tr}(xd_n)) : x \in \mathbb{F}_q\},$$

where Tr denotes the absolute trace function over \mathbb{F}_q . The set D is called the defining set of this code \mathcal{C}_D . This construction was proposed by Ding et al. (see [4, 9]) and is used to obtain linear codes with few weights [10, 16, 17, 20].

In this paper, we set

$$\begin{aligned} D &= \{x \in \mathbb{F}_q^* : \text{Tr}(x^2 + x) = 0\} = \{d_1, d_2, \dots, d_n\}, \\ \mathcal{C}_D &= \{\mathbf{c}_x = (\text{Tr}(xd_1), \text{Tr}(xd_2), \dots, \text{Tr}(xd_n)) : x \in \mathbb{F}_q\} \end{aligned} \quad (1.1)$$

and determine the weight distribution of the proposed linear codes \mathcal{C}_D of (1.1).

The parameters of the introduced linear codes \mathcal{C}_D of (1.1) are described in the following theorems. The proofs of the parameters will be presented later.

Table 1: The weight distribution of the codes of Theorem 1

Weight w	Multiplicity A
0	1
$(p-1)p^{m-2}$	$p^{m-2} - 1 + p^{-1}(p-1)G$
$(p-1)p^{m-2} + p^{-1}(p-1)G$	$2(p-1)p^{m-2} - p^{-1}(p-1)G$
$(p-1)p^{m-2} + p^{-1}(p-2)G$	$(p-1)^2p^{m-2}$

Theorem 1 Let $m > 2$ be even with $p \mid m$. Then the code \mathcal{C}_D of (1.1) is a $[p^{m-1} - 1 + p^{-1}(p-1)G, m]$ linear code with weight distribution in Table 1, where $G = -(-1)^{\frac{m(p-1)}{4}} p^{\frac{m}{2}}$.

Example 2 Let $(p, m) = (3, 6)$. Then the corresponding code \mathcal{C}_D has parameters $[260, 6, 162]$ and weight enumerator $1 + 98x^{162} + 324x^{171} + 306x^{180}$.

Theorem 3 Let m be even with $p \nmid m$. Then the code \mathcal{C}_D of (1.1) is a $[p^{m-1} - p^{-1}G - 1, m]$ linear code with weight distribution in Table 2, where $G = -(-1)^{\frac{m(p-1)}{4}} p^{\frac{m}{2}}$.

Example 4 Let $(p, m) = (3, 4)$. Then the corresponding code \mathcal{C}_D has parameters $[29, 4, 18]$ and weight enumerator $1 + 44x^{18} + 30x^{21} + 6x^{24}$. This code is optimal according to the codetables in [11].

Table 2: The weight distribution of the codes of Theorem 3.

Weight w	Multiplicity A
0	1
$(p-1)p^{m-2} - p^{-1}G$	$(p-1)(2p^{m-2} + p^{-1}G)$
$(p-1)p^{m-2}$	$\frac{1}{2}(p-1)(p^{m-1} - G) + p^{m-2} - 1$
$(p-1)p^{m-2} - 2p^{-1}G$	$\frac{1}{2}(p^2 - 3p + 2)(p^{m-2} + p^{-1}G)$

Table 3: The weight distribution of the codes of Theorem 5.

Weight w	Multiplicity A
0	1
$(p-1)p^{m-2}$	$p^{m-1} - 1$
$(p-1)p^{m-2} + p^{\frac{m-3}{2}}$	$\frac{1}{2}(p-1)^2 p^{m-2}$
$(p-1)p^{m-2} - p^{\frac{m-3}{2}}$	$\frac{1}{2}(p-1)^2 p^{m-2}$
$(p-1)p^{m-2} - (p-1)p^{\frac{m-3}{2}}$	$\frac{1}{2}(p-1)(p^{m-2} + p^{\frac{m-1}{2}})$
$(p-1)p^{m-2} + (p-1)p^{\frac{m-3}{2}}$	$\frac{1}{2}(p-1)(p^{m-2} - p^{\frac{m-1}{2}})$

Theorem 5 If m is odd and $p \mid m$, then the linear code \mathcal{C}_D of (1.1) has parameters $[p^{m-1} - 1, m]$ and weight distribution in Table 3.

Example 6 Let $(p, m) = (3, 3)$. Then the corresponding code \mathcal{C}_D has parameters $[8, 3, 4]$ and weight enumerator $1 + 6x^4 + 6x^5 + 8x^6 + 6x^7$. This code is almost optimal, since the optimal linear code has parameters $[8, 3, 5]$. By Table 3, \mathcal{C}_D in Theorem 5 is a four weight linear code if and only if $p = m = 3$.

Example 7 Let $(p, m) = (5, 5)$. Then the corresponding code \mathcal{C}_D has parameters $[624, 5, 480]$ and weight enumerator $1 + 300x^{480} + 1000x^{495} + 624x^{500} + 1000x^{505} + 200x^{520}$.

Table 4: The weight distribution of the codes of Theorem 8.

Weight w	Multiplicity A
0	1
$(p-1)p^{m-2} + \frac{1}{p}(\frac{-m}{p})G\overline{G}$	$(p-1)(p^{m-2} - p^{-2}(\frac{-m}{p})G\overline{G})$
$(p-1)p^{m-2}$	$p^{m-2} + p^{-2}(\frac{-m}{p})(p-1)G\overline{G} - 1$
$(p-1)p^{m-2} + (\frac{-m}{p})p^{-2}(p-1)G\overline{G}$	$\frac{1}{2}(p-1)(p^{m-1} - (\frac{-m}{p})p^{-1}G\overline{G})$
$(p-1)p^{m-2} + (\frac{-m}{p})p^{-2}(p+1)G\overline{G}$	$\frac{1}{2}(p-1)(p-2)(p^{m-2} - (\frac{-m}{p})p^{-2}G\overline{G})$
$(p-1)p^{m-2} + p^{-2}(\frac{-m}{p})G\overline{G}$	$(p-1)p^{m-2} + p^{-2}(\frac{-m}{p})(p-1)^2G\overline{G}$

Theorem 8 *If m is odd and $p \nmid m$, then the linear code \mathcal{C}_D of (1.1) has parameters $[p^{m-1} + p^{-1}(\frac{-m}{p})G\overline{G} - 1, m]$ and weight distribution in Table 4, where (\cdot) is the Legendre symbol and $G\overline{G} = (-1)^{\frac{(m+1)(p-1)}{4}}p^{\frac{m+1}{2}}$.*

Example 9 *Let $(p, m) = (3, 5)$. Then the corresponding code \mathcal{C}_D has parameters $[71, 5, 42]$ and weight enumerator $1 + 30x^{42} + 60x^{45} + 90x^{48} + 42x^{51} + 20x^{54}$. We remark that this linear code is near optimal, since the corresponding optimal linear codes has parameters $[71, 5, 42]$.*

Remark: In Theorem 8, if $m = 3$ and $p \equiv 2 \pmod{3}$, the frequency of weight $(p-1)p^{m-2}$ turns to be zero. Hence, in this case \mathcal{C}_D is a four-weight linear code with weight distribution in Table 5.

Example 10 *Let $(p, m) = (5, 3)$. Then the corresponding code \mathcal{C}_D has parameters $[19, 3, 14]$ and weight enumerator $1 + 36x^{14} + 24x^{15} + 60x^{16} + 4x^{19}$. This code is optimal according to the datatables in [11].*

Table 5: The weight distribution of \mathcal{C}_D , when $m = 3$ and $p \equiv 2 \pmod{3}$.

Weight w	Multiplicity A
0	1
$p^2 - 2p$	$p^2 - 1$
$p^2 - 2p + 1$	$\frac{1}{2}p(p^2 - 1)$
$p^2 - 2p - 1$	$\frac{1}{2}(p-2)(p^2 - 1)$
$p^2 - p - 1$	$p - 1$

2 Preliminaries

In this section, we review some basic notations and results of group characters and present some lemma which are needed for the proof of the main results.

An additive character χ of \mathbb{F}_q is a mapping from \mathbb{F}_q into the multiplicative group of complex numbers of absolute value 1 with $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in \mathbb{F}_q$ [15].

By Theorem 5.7 in [15], for $b \in \mathbb{F}_q$,

$$\chi_b(x) = e^{\frac{2\pi\sqrt{-1}\text{Tr}(bx)}{p}}, \quad \text{for all } x \in \mathbb{F}_q \quad (2.1)$$

defines an additive character of \mathbb{F}_q , and all additive characters can be obtained in this way. Among the additive characters, we have the *trivial character* χ_0 defined by $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q$; all other characters are called *nontrivial*. The character χ_1 in (2.1) will be called the *canonical additive character* of \mathbb{F}_q [15].

The orthogonal property of additive characters can be found in [15] and is given as below

$$\sum_{x \in \mathbb{F}_q} \chi(x) = \begin{cases} q, & \text{if } \chi \text{ is trivial,} \\ 0, & \text{if } \chi \text{ is nontrivial.} \end{cases}$$

Characters of the *multiplicative group* \mathbb{F}_q^* of \mathbb{F}_q are called multiplicative character of \mathbb{F}_q . By Theorem 5.8 in [15], for each $j = 0, 1, \dots, q-2$, the function ψ_j with

$$\psi_j(g^k) = e^{2\pi\sqrt{-1}jk/(q-1)} \text{ for } k = 0, 1, \dots, q-2$$

defines a multiplicative character of \mathbb{F}_q , where g is a generator of \mathbb{F}_q^* . For $j = (q-1)/2$, we have the *quadratic character* $\eta = \psi_{(q-1)/2}$ defined by

$$\eta(g^k) = \begin{cases} -1, & \text{if } 2 \nmid k, \\ 1, & \text{if } 2 \mid k. \end{cases}$$

In the sequel, we assume that $\eta(0) = 0$.

We define the quadratic Gauss sum $G = G(\eta, \chi_1)$ over \mathbb{F}_q by

$$G(\eta, \chi_1) = \sum_{x \in \mathbb{F}_q^*} \eta(x) \chi_1(x),$$

and the quadratic Gauss sum $\overline{G} = G(\overline{\eta}, \overline{\chi}_1)$ over \mathbb{F}_p by

$$G(\overline{\eta}, \overline{\chi}_1) = \sum_{x \in \mathbb{F}_p^*} \overline{\eta}(x) \overline{\chi}_1(x),$$

where $\overline{\eta}$ and $\overline{\chi}_1$ denote the quadratic and canonical character of \mathbb{F}_p , respectively.

The explicit values of quadratic Gauss sums are given as follows.

Lemma 11 ([15], Theorem 5.15) *Let the symbols be the same as before. Then*

$$G(\eta, \chi_1) = (-1)^{(m-1)} \sqrt{-1}^{\frac{(p-1)^2 m}{4}} \sqrt{q}, \quad G(\overline{\eta}, \overline{\chi}_1) = \sqrt{-1}^{\frac{(p-1)^2}{4}} \sqrt{p}.$$

Lemma 12 ([9], Lemma 7) *Let the symbols be the same as before. Then*

1. if $m \geq 2$ is even, then $\eta(y) = 1$ for each $y \in \mathbb{F}_p^*$;
2. if m is odd, then $\eta(y) = \overline{\eta}(y)$ for each $y \in \mathbb{F}_p^*$.

Lemma 13 ([15], **Theorem 5.33**) *Let χ be a nontrivial additive character of \mathbb{F}_q , and let $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$ with $a_2 \neq 0$. Then*

$$\sum_{x \in \mathbb{F}_q} \chi(f(x)) = \chi(a_0 - a_1^2(4a_2)^{-1}) \eta(a_2) G(\eta, \chi).$$

Lemma 14 *Let the symbols be the same as before. For $y \in F_p^*$, we have*

$$\sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y \text{Tr}(x^2+x)} = \begin{cases} (p-1)G, & \text{if } 2 \mid m \text{ and } p \mid m, \\ -G, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ 0, & \text{if } 2 \nmid m \text{ and } p \mid m, \\ \bar{\eta}(-m)G\bar{G}, & \text{if } 2 \mid m \text{ and } p \nmid m. \end{cases}$$

Proof It follows from Lemma 13 that

$$\begin{aligned} \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y \text{Tr}(x^2+x)} &= \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \chi_1(yx^2 + yx) \\ &= G \sum_{y \in \mathbb{F}_p^*} \chi_1\left(-\frac{y}{4}\right) \eta(y) \\ &= G \sum_{y \in \mathbb{F}_p^*} \eta(y) \zeta_p^{-\frac{y \text{Tr}(1)}{4}}. \end{aligned}$$

It is obviously that

$$\text{Tr}(1) = m = \begin{cases} 0, & \text{if } p \mid m, \\ \neq 0, & \text{otherwise.} \end{cases}$$

Consequently,

$$\sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y \text{Tr}(x^2+x)} = \begin{cases} G \sum_{y \in \mathbb{F}_p^*} \eta(y), & \text{if } 2 \mid m \text{ and } p \mid m, \\ G \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-\frac{ym}{4}}, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ G \sum_{y \in \mathbb{F}_p^*} \eta(y), & \text{if } 2 \nmid m \text{ and } p \mid m, \\ \eta(-m)G \sum_{y \in \mathbb{F}_p^*} \eta\left(-\frac{ym}{4}\right) \zeta_p^{-\frac{ym}{4}}, & \text{if } 2 \nmid m \text{ and } p \nmid m. \end{cases}$$

Using Lemma 12, we get this lemma.

Lemma 15 *Let the symbols be the same as before. For $b \in F_q^*$, let*

$$B = \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \chi_1(yx^2 + yx + bzx).$$

Then

1. *if $\text{Tr}(b^2) \neq 0$ and $\text{Tr}(b) = 0$, we have*

$$B = \begin{cases} -(p-1)G, & \text{if } 2 \mid m \text{ and } p \mid m, \\ \bar{\eta}(m \text{Tr}(b^2)) G\bar{G}^2 + G, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ \bar{\eta}(-\text{Tr}(b^2)) (p-1)G\bar{G}, & \text{if } 2 \nmid m \text{ and } p \mid m, \\ -\bar{\eta}(-\text{Tr}(b^2)) + \bar{\eta}(-m) G\bar{G}, & \text{if } 2 \nmid m \text{ and } p \nmid m; \end{cases}$$

2. if $\text{Tr}(b^2) \neq 0$ and $\text{Tr}(b) \neq 0$, we have

$$B = \begin{cases} \bar{\eta}(-1)G\bar{G}^2 - (p-1)G, & \text{if } 2 \mid m \text{ and } p \mid m, \\ G, & \text{if } 2 \mid m, p \nmid m \text{ and } (\text{Tr}(b))^2 = m\text{Tr}(b^2), \\ \bar{\eta}(m\text{Tr}(b^2) - (\text{Tr}(b))^2)G\bar{G}^2 + G, & \text{if } 2 \mid m, p \nmid m \text{ and } (\text{Tr}(b))^2 \neq m\text{Tr}(b^2), \\ -\bar{\eta}(-\text{Tr}(b^2))G\bar{G}, & \text{if } 2 \nmid m \text{ and } p \mid m, \\ (\bar{\eta}(-\text{Tr}(b^2))(p-1) - \bar{\eta}(-m))G\bar{G}, & \text{if } 2 \nmid m, p \nmid m \text{ and } (\text{Tr}(b))^2 = m\text{Tr}(b^2), \\ -(\bar{\eta}(-\text{Tr}(b^2)) + \bar{\eta}(-m))G\bar{G}, & \text{if } 2 \nmid m, p \nmid m \text{ and } (\text{Tr}(b))^2 \neq m\text{Tr}(b^2); \end{cases}$$

3. if $\text{Tr}(b^2) = 0$ and $\text{Tr}(b) \neq 0$, we have

$$B = \begin{cases} -(p-1)G, & \text{if } 2 \mid m \text{ and } p \mid m, \\ G, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ 0, & \text{if } 2 \nmid m \text{ and } p \mid m, \\ -\bar{\eta}(-m)G\bar{G}, & \text{if } 2 \nmid m \text{ and } p \nmid m; \end{cases}$$

4. if $\text{Tr}(b^2) = 0$ and $\text{Tr}(b) = 0$, we have

$$B = \begin{cases} (p-1)^2G, & \text{if } 2 \mid m \text{ and } p \mid m, \\ -(p-1)G, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ 0, & \text{if } 2 \nmid m \text{ and } p \mid m, \\ \bar{\eta}(-m)(p-1)G\bar{G}, & \text{if } 2 \nmid m \text{ and } p \nmid m. \end{cases}$$

Proof We only give the proof of the first part since the remaining parts are similar.

By Lemma 13, we have

$$\begin{aligned} B &= G \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \eta(y) \chi_1 \left(-\frac{(y+bz)^2}{4y} \right) \\ &= G \sum_{y \in \mathbb{F}_p^*} \eta(y) \chi_1 \left(-\frac{y}{4} \right) \sum_{z \in \mathbb{F}_p^*} \chi_1 \left(-\frac{b^2 z^2}{4y} - \frac{bz}{2} \right) \\ &= G \sum_{y \in \mathbb{F}_p^*} \eta(y) \chi_1 \left(-\frac{y}{4} \right) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-\frac{\text{Tr}(b^2)z^2}{4y} - \frac{\text{Tr}(b)z}{2}}. \end{aligned}$$

Note that in the first part, $\text{Tr}(b^2) \neq 0$ and $\text{Tr}(b) = 0$. Therefore,

$$\begin{aligned}
B &= G \sum_{y \in \mathbb{F}_p^*} \eta(y) \chi_1 \left(-\frac{y}{4} \right) \sum_{z \in \mathbb{F}_p^*} \bar{\chi}_1 \left(-\frac{\text{Tr}(b^2)z^2}{4y} \right) \\
&= G \sum_{y \in \mathbb{F}_p^*} \eta(y) \chi_1 \left(-\frac{y}{4} \right) \sum_{z \in \mathbb{F}_p^*} \bar{\chi}_1 \left(-\frac{\text{Tr}(b^2)z^2}{4y} \right) - G \sum_{y \in \mathbb{F}_p^*} \eta(y) \chi_1 \left(-\frac{y}{4} \right) \\
&= G \sum_{y \in \mathbb{F}_p^*} \eta(y) \chi_1 \left(-\frac{y}{4} \right) \bar{\chi}_1(0) \bar{\eta}(-\text{Tr}(b^2)y) \bar{G} - G \sum_{y \in \mathbb{F}_p^*} \eta(y) \chi_1 \left(-\frac{y}{4} \right) \\
&= \bar{\eta}(-\text{Tr}(b^2)) G \bar{G} \sum_{y \in \mathbb{F}_p^*} \eta(y) \chi_1 \left(-\frac{y}{4} \right) \bar{\eta}(y) - G \sum_{y \in \mathbb{F}_p^*} \eta(y) \chi_1 \left(-\frac{y}{4} \right) \\
&= \begin{cases} \bar{\eta}(-\text{Tr}(b^2)) G \bar{G} \sum_{y \in \mathbb{F}_p^*} \bar{\eta}(y) - G \sum_{y \in \mathbb{F}_p^*} 1, & \text{if } 2 \mid m \text{ and } p \mid m, \\ \bar{\eta}(m \text{Tr}(b^2)) G \bar{G} \sum_{y \in \mathbb{F}_p^*} \bar{\chi}_1 \left(-\frac{my}{4} \right) \bar{\eta} \left(-\frac{my}{4} \right) - G \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-\frac{my}{4}}, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ \bar{\eta}(-\text{Tr}(b^2)) G \bar{G} \sum_{y \in \mathbb{F}_p^*} 1 - G \sum_{y \in \mathbb{F}_p^*} \bar{\eta}(y), & \text{if } 2 \nmid m \text{ and } p \mid m, \\ \bar{\eta}(-\text{Tr}(b^2)) G \bar{G} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-\frac{my}{4}} - G \bar{\eta}(-m) \sum_{y \in \mathbb{F}_p^*} \bar{\eta} \left(-\frac{my}{4} \right) \zeta_p^{-\frac{my}{4}}, & \text{if } 2 \nmid m \text{ and } p \nmid m. \end{cases}
\end{aligned}$$

Combining Lemma 12 and the equation $\sum_{y \in \mathbb{F}_p^*} \zeta_p^y = -1$, we get the result of the first part.

Lemma 16 For $a \in \mathbb{F}_p$, let

$$N(0, a) = \{x \in F_q : \text{Tr}(x^2) = 0, \text{Tr}(x) = a\}.$$

Then

1. if $a \neq 0$, we have

$$|N(0, a)| = \begin{cases} p^{m-2}, & \text{if } p \mid m, \\ p^{m-2} + p^{-1}G, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ p^{m-2} - p^{-2}\bar{\eta}(-m)G\bar{G}, & \text{if } 2 \nmid m \text{ and } p \nmid m; \end{cases}$$

2. if $a = 0$, we have

$$|N(0, 0)| = \begin{cases} p^{m-2} + p^{-1}(p-1)G, & \text{if } 2 \mid m \text{ and } p \mid m, \\ p^{m-2}, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ p^{m-2}, & \text{if } 2 \nmid m \text{ and } p \mid m, \\ p^{m-2} + p^{-2}\bar{\eta}(-m)(p-1)G\bar{G}, & \text{if } 2 \nmid m \text{ and } p \nmid m. \end{cases}$$

Proof We only prove the first statement of this lemma, since the other statements can be similarly proved.

For $a \in \mathbb{F}_p^*$, we have

$$\begin{aligned}
|N(0, a)| &= p^{-2} \sum_{x \in \mathbb{F}_q} \left(\sum_{y \in F_p} \zeta_p^{y \text{Tr}(x^2)} \right) \left(\sum_{z \in F_p} \zeta_p^{z(\text{Tr}(x) - a)} \right) \\
&= p^{-2} \sum_{x \in \mathbb{F}_q} \left(1 + \sum_{y \in F_p^*} \zeta_p^{y \text{Tr}(x^2)} \right) \left(1 + \sum_{z \in F_p^*} \zeta_p^{z(\text{Tr}(x) - a)} \right) \\
&= p^{m-2} + p^{-2} \sum_{y \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y \text{Tr}(x^2)} + p^{-2} \sum_{z \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{z(\text{Tr}(x) - a)} \\
&\quad + p^{-2} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(yx^2 + zx) - za} \\
&= p^{m-2} + p^{-2} \sum_{y \in F_p^*} \sum_{x \in \mathbb{F}_q} \chi_1(yx^2) + p^{-2} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \sum_{x \in \mathbb{F}_q} \chi_1(yx^2 + zx).
\end{aligned}$$

By Lemma 13, we obtain

$$\begin{aligned}
|N(0, a)| &= p^{m-2} + p^{-2} \sum_{y \in F_p^*} \sum_{x \in \mathbb{F}_q} \chi_1(yx^2) + p^{-2} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \sum_{x \in \mathbb{F}_q} \chi_1(yx^2 + zx) \\
&= p^{m-2} + p^{-2} \sum_{y \in F_p^*} \chi_1(0) \eta(y) G + p^{-2} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \chi_1\left(-\frac{z^2}{4y}\right) \eta(y) G \\
&= \begin{cases} p^{m-2} + p^{-2} G \sum_{y \in F_p^*} \eta(y) + p^{-2} G \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \eta(y), & \text{if } p \mid m \\ p^{m-2} + p^{-2} G \sum_{y \in F_p^*} \eta(y) + p^{-2} G \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \eta(y) \zeta_p^{-\frac{mz^2}{4y}}, & \text{if } p \nmid m \end{cases} \\
&= \begin{cases} p^{m-2}, & \text{if } p \mid m \\ p^{m-2} + p^{-2}(p-1)G + p^{-2} G \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \zeta_p^{-\frac{mz^2}{4y}}, & \text{if } 2 \mid m \text{ and } p \nmid m \\ p^{m-2} + p^{-2} \eta(-m) G \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-za} \eta\left(-\frac{mz^2}{4y}\right) \zeta_p^{-\frac{mz^2}{4y}}, & \text{if } 2 \nmid m \text{ and } p \nmid m \end{cases} \\
&= \begin{cases} p^{m-2}, & \text{if } p \mid m, \\ p^{m-2} + p^{-1} G, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ p^{m-2} - p^{-2} \bar{\eta}(-m) G \bar{G}, & \text{if } 2 \nmid m \text{ and } p \nmid m. \end{cases}
\end{aligned}$$

Lemma 17 *Let*

$$N(0, \bar{0}) = \{x \in F_q : \text{Tr}(x^2) = 0 \text{ and } \text{Tr}(x) \neq 0\},$$

$$N(\bar{0}, \bar{0}) = \{x \in F_q : \text{Tr}(x^2) \neq 0 \text{ and } \text{Tr}(x) \neq 0\},$$

$$N(\bar{0}, 0) = \{x \in F_q : \text{Tr}(x^2) \neq 0 \text{ and } \text{Tr}(x) = 0\}.$$

Then we get

1.

$$|N(0, \bar{0})| = \begin{cases} (p-1)p^{m-2}, & \text{if } p \mid m, \\ (p-1)(p^{m-2} + p^{-1}G), & \text{if } 2 \mid m \text{ and } p \nmid m, \\ (p-1)(p^{m-2} - p^{-2} \bar{\eta}(-m) G \bar{G}), & \text{if } 2 \nmid m \text{ and } p \nmid m; \end{cases}$$

2.

$$|N(\bar{0}, \bar{0})| = \begin{cases} (p-1)^2 p^{m-2}, & \text{if } p \mid m, \\ (p-1)^2 p^{m-2} - (p-1)p^{-1}G, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ (p-1)^2 p^{m-2} + (p-1)p^{-2}\bar{\eta}(-m)G\bar{G}, & \text{if } 2 \nmid m \text{ and } p \nmid m; \end{cases}$$

3.

$$|N(\bar{0}, 0)| = \begin{cases} (p-1)p^{m-2} - p^{-1}(p-1)G, & \text{if } 2 \mid m \text{ and } p \mid m, \\ (p-1)p^{m-2}, & \text{if } 2 \mid m \text{ and } p \nmid m, \\ (p-1)p^{m-2}, & \text{if } 2 \nmid m \text{ and } p \mid m, \\ (p-1)p^{m-2} - p^{-2}\bar{\eta}(-m)(p-1)G\bar{G}, & \text{if } 2 \nmid m \text{ and } p \nmid m. \end{cases}$$

Proof By the definitions, we have

$$|N(\bar{0}, 0)| + |N(0, 0)| = p^{m-1},$$

$$|N(0, \bar{0})| = \sum_{a \in F_p^*} |N(0, a)|,$$

$$|N(\bar{0}, \bar{0})| + |N(0, \bar{0})| = p^m - p^{m-1}.$$

Then the desired results follow from Lemma 16.

Lemma 18 Suppose $p \nmid m$ and let

$$V = \{x \in F_q : \text{Tr}(x) \neq 0 \text{ and } (\text{Tr}(x))^2 = m\text{Tr}(x^2)\}.$$

Then

$$|V| = \begin{cases} (p-1)p^{m-2}, & \text{if } 2 \mid m, \\ (p-1)p^{m-2} + p^{-2}\bar{\eta}(-m)(p-1)^2G\bar{G}, & \text{if } 2 \nmid m. \end{cases}$$

Proof For $c \in \mathbb{F}_p^*$, set

$$S_c = \{x \in \mathbb{F}_p : \text{Tr}(x) = c \text{ and } \text{Tr}(x^2) = c^2/m\}.$$

Then

$$|V| = \sum_{c \in F_p^*} |S_c|.$$

By definition, we have

$$\begin{aligned} |S_c| &= p^{-2} \sum_{x \in \mathbb{F}_q} \left(\sum_{y \in F_p} \zeta_p^{y(\text{Tr}(x^2) - \frac{c^2}{m})} \right) \left(\sum_{z \in F_p} \zeta_p^{z(\text{Tr}(x) - c)} \right) \\ &= p^{-2} \sum_{x \in \mathbb{F}_q} \left(1 + \sum_{y \in F_p^*} \zeta_p^{y(\text{Tr}(x^2) - \frac{c^2}{m})} \right) \left(1 + \sum_{z \in F_p^*} \zeta_p^{z(\text{Tr}(x) - c)} \right) \\ &= p^{m-2} + p^{-2} \sum_{y \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y(\text{Tr}(x^2) - \frac{c^2}{m})} + p^{-2} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(yx^2 + zx) - \frac{yc^2}{m} - zc}. \end{aligned}$$

Let

$$s_c = \sum_{y \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y \left(\text{Tr}(x^2) - \frac{c^2}{m} \right)},$$

$$\bar{s}_c = \sum_{y \in F_p^*} \sum_{z \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(yx^2 + zx) - \frac{yc^2}{m} - zc}.$$

It is straightforward to have that

$$s_c = \sum_{y \in F_p^*} \zeta_p^{-\frac{yc^2}{m}} \sum_{x \in \mathbb{F}_q} \chi_1(yx^2).$$

By Lemma 13, we obtain

$$\begin{aligned} s_c &= \sum_{y \in F_p^*} \zeta_p^{-\frac{yc^2}{m}} \chi_1(0) \eta(y) G \\ &= \begin{cases} G \sum_{y \in F_p^*} \zeta_p^{-\frac{yc^2}{m}}, & \text{if } 2 \mid m \\ \eta(-m) G \sum_{y \in F_p^*} \eta\left(-\frac{yc^2}{m}\right) \zeta_p^{-\frac{yc^2}{m}}, & \text{if } 2 \nmid m \end{cases} \\ &= \begin{cases} -G, & \text{if } 2 \mid m, \\ \bar{\eta}(-m) G \bar{G}, & \text{if } 2 \nmid m. \end{cases} \end{aligned} \quad (2.2)$$

Meanwhile,

$$\begin{aligned} \bar{s}_c &= \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-\frac{yc^2}{m} - zc} \sum_{x \in \mathbb{F}_q} \chi_1(yx^2 + zx) \\ &= \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-\frac{yc^2}{m} - zc} \chi_1\left(-\frac{z^2}{4y}\right) \eta(y) G. \end{aligned}$$

Hence,

$$\begin{aligned} \sum_{c \in F_p^*} \bar{s}_c &= G \sum_{y \in F_p^*} \sum_{z \in F_p^*} \chi_1\left(-\frac{z^2}{4y}\right) \eta(y) \sum_{c \in F_p^*} \zeta_p^{-\frac{yc^2}{m} - zc} \\ &= G \sum_{y \in F_p^*} \sum_{z \in F_p^*} \chi_1\left(-\frac{z^2}{4y}\right) \eta(y) \sum_{c \in F_p} \bar{\chi}_1\left(-\frac{yc^2}{m} - zc\right) - G \sum_{y \in F_p^*} \sum_{z \in F_p^*} \chi_1\left(-\frac{z^2}{4y}\right) \eta(y) \\ &= G \sum_{y \in F_p^*} \sum_{z \in F_p^*} \chi_1\left(-\frac{z^2}{4y}\right) \eta(y) \bar{\chi}_1\left(\frac{mz^2}{4y}\right) \bar{\eta}(-my) \bar{G} - G \sum_{y \in F_p^*} \sum_{z \in F_p^*} \chi_1\left(-\frac{z^2}{4y}\right) \eta(y) \\ &= \bar{\eta}(-m) G \bar{G} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \eta(y) \bar{\eta}(y) - G \sum_{y \in F_p^*} \sum_{z \in F_p^*} \zeta_p^{-\frac{mz^2}{4y}} \eta(y) \\ &= \begin{cases} (p-1)G, & \text{if } 2 \mid m, \\ \bar{\eta}(-m)(p-1)^2 G \bar{G} - \bar{\eta}(-m)(p-1) G \bar{G}, & \text{if } 2 \nmid m. \end{cases} \end{aligned} \quad (2.3)$$

We get

$$\begin{aligned} |V| &= \sum_{c \in F_p^*} |S_c| = \sum_{c \in F_p^*} (p^{m-2} + p^{-2}s_c + p^{-2}\bar{s}_c) \\ &= \sum_{c \in F_p^*} p^{m-2} + p^{-2} \sum_{c \in F_p^*} s_c + p^{-2} \sum_{c \in F_p^*} \bar{s}_c. \end{aligned}$$

By (2.2) and (2.3), we get this lemma.

3 Proof of main results

In this section, we will present a class of linear codes with three weights and five weights over \mathbb{F}_p .

Recall that the defining set considered in this paper is defined by

$$D = \{x \in \mathbb{F}_q^* : \text{Tr}(x^2 + x) = 0\}.$$

Let $n_0 = |D| + 1$. Then

$$\begin{aligned} n_0 &= \frac{1}{p} \sum_{x \in F_q} \left(\sum_{y \in F_p} \zeta_p^{y \text{Tr}(x^2+x)} \right) \\ &= p^{m-1} + \frac{1}{p} \sum_{x \in F_q} \sum_{y \in F_p^*} \zeta_p^{y \text{Tr}(x^2+x)}. \end{aligned}$$

Define $N_b = \{x \in \mathbb{F}_q : \text{Tr}(x^2 + x) = 0 \text{ and } \text{Tr}(bx) = 0\}$. Let $\text{wt}(\mathbf{c}_b)$ denote the Hamming weight of the codeword \mathbf{c}_b of the code \mathcal{C}_D . It can be easily checked that

$$\text{wt}(\mathbf{c}_b) = n_0 - |N_b|. \quad (3.1)$$

For $b \in \mathbb{F}_q^*$, we have

$$\begin{aligned} |N_b| &= p^{-2} \sum_{x \in \mathbb{F}_q} \left(\sum_{y \in F_p} \zeta_p^{y \text{Tr}(x^2+x)} \right) \left(\sum_{z \in F_p} \zeta_p^{z \text{Tr}(bx)} \right) \\ &= p^{-2} \sum_{x \in \mathbb{F}_q} \left(1 + \sum_{y \in F_p^*} \zeta_p^{y \text{Tr}(x^2+x)} \right) \left(1 + \sum_{z \in F_p^*} \zeta_p^{z \text{Tr}(bx)} \right) \\ &= p^{m-2} + p^{-2} \sum_{y \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y \text{Tr}(x^2+x)} + p^{-2} \sum_{z \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{z \text{Tr}(bx)} \\ &\quad + p^{-2} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(yx^2+yx+bzx)} \\ &= p^{m-2} + p^{-2} \sum_{y \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{y \text{Tr}(x^2+x)} + p^{-2} \sum_{y \in F_p^*} \sum_{z \in F_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}(yx^2+yx+bzx)}. \end{aligned} \quad (3.2)$$

Our task in this section is to calculate n_0 , $|N_b|$ and give the proof of the main results.

3.1 The first case of three-weight linear codes

In this subsection, suppose $2 \mid m$ and $p \mid m$. To determine the weight distribution of \mathcal{C}_D of (1.1), the following lemma is needed.

Lemma 19 *Let $b \in \mathbb{F}_q^*$. Then*

$$|N_b| = \begin{cases} p^{m-2}, & \text{if } \text{Tr}(b^2) = 0 \text{ and } \text{Tr}(b) \neq 0 \\ & \text{or } \text{Tr}(b^2) \neq 0 \text{ and } \text{Tr}(b) = 0, \\ p^{m-2} - (-1)^{\frac{m(p-1)}{4}}(p-1)p^{\frac{m-2}{2}}, & \text{if } \text{Tr}(b^2) = 0 \text{ and } \text{Tr}(b) = 0, \\ p^{m-2} - (-1)^{\frac{m(p-1)}{4}}p^{\frac{m-2}{2}}, & \text{if } \text{Tr}(b^2) \neq 0 \text{ and } \text{Tr}(b) \neq 0. \end{cases}$$

Proof The desired result follows directly from (3.2), Lemmas 11, 14 and 15. We omit the details.

After the preparations above, we proceed to prove Theorem 1. By Lemma 14, if $2 \mid m$ and $p \mid m$, we have

$$n_0 = p^{m-1} + p^{-1}(p-1)G.$$

Combining (3.1), (3.2) and Lemma 19, we get

$$\begin{aligned} \text{wt}(c_b) &= n_0 - |N_b| \\ &\in \{(p-1)p^{m-2} + p^{-1}(p-1)G, (p-1)p^{m-2}, (p-1)p^{m-2} + p^{-1}(p-2)G\}. \end{aligned}$$

Set

$$\begin{aligned} \omega_1 &= (p-1)p^{m-2} + p^{-1}(p-1)G, \\ \omega_2 &= (p-1)p^{m-2}, \\ \omega_3 &= (p-1)p^{m-2} + p^{-1}(p-2)G. \end{aligned}$$

By Lemma 19, we obtain

$$\begin{aligned} A_{\omega_1} &= |N(0, \bar{0})| + |N(\bar{0}, 0)|, \\ A_{\omega_2} &= |N(0, 0)| - 1, \\ A_{\omega_3} &= |N(\bar{0}, \bar{0})|. \end{aligned}$$

Then the results in Theorem 1 follow from Lemmas 11 and 17.

3.2 The second case of three-weight linear codes

In this subsection, assume $2 \mid m$ and $p \nmid m$. By (3.2), Lemmas 14 and 15, it is easy to get the following lemma.

Lemma 20 *Let $b \in \mathbb{F}_q^*$ and the symbols be the same as before. Then we have*

$$|N_b| = \begin{cases} p^{m-2}, & \text{if } \text{Tr}(b^2) = 0 \text{ and } \text{Tr}(b) \neq 0 \text{ or} \\ & \text{Tr}(b^2) \neq 0 \text{ and } (\text{Tr}(b))^2 = m\text{Tr}(b^2), \\ p^{m-2} - p^{-1}G, & \text{if } \text{Tr}(b^2) = 0 \text{ and } \text{Tr}(b) = 0, \\ p^{m-2} + p^{-2}\bar{\eta}(m\text{Tr}(b^2) - (\text{Tr}(b))^2)G\bar{G}^2, & \text{if } \text{Tr}(b^2) \neq 0 \text{ and } (\text{Tr}(b))^2 \neq m\text{Tr}(b^2), \\ p^{m-2} + p^{-2}\bar{\eta}(m\text{Tr}(b^2))G\bar{G}^2, & \text{if } \text{Tr}(b^2) \neq 0 \text{ and } \text{Tr}(b) = 0. \end{cases}$$

We are now turning to the proof of Theorem 3. If $2 \mid m$ and $p \nmid m$, by Lemma 14, we have

$$n_0 = p^{m-1} - p^{-1}G.$$

It follows from (3.1) and Lemma 20 that

$$wt(c_b) \in \{(p-1)p^{m-2} - p^{-1}G, (p-1)p^{m-2}, (p-1)p^{m-2} - 2p^{-1}G\}.$$

Suppose

$$\begin{aligned} \omega_1 &= (p-1)p^{m-2} - p^{-1}G, \\ \omega_2 &= (p-1)p^{m-2}, \\ \omega_3 &= (p-1)p^{m-2} - 2p^{-1}G. \end{aligned}$$

By Lemmas 17, 18 and 20, we have

$$A_{\omega_1} = |N(0, \bar{0})| + |V| = (p-1)(2p^{m-2} + p^{-1}G).$$

It is easy to check that the minimum distance of the dual code \mathcal{C}_D^\perp of \mathcal{C}_D is equal to 2. By the first two Pless Power Moments([12], p. 260) the frequency A_{w_i} of w_i satisfies the following equations:

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} = p^m - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_3} = p^{m-1}(p-1)n, \end{cases} \quad (3.3)$$

where $n = p^{m-1} - p^{-1}G - 1$. A simple calculation leads to the weight distribution of Table 2. The proof of Theorem 3 is completed.

3.3 The first case of 5-weight linear codes

In this subsection, set $2 \nmid m$ and $p \mid m$. By (3.2), Lemmas 14 and 15, we get the following lemma.

Lemma 21 *Let $b \in \mathbb{F}_q^*$, then*

$$|N_b| = \begin{cases} p^{m-2}, & \text{if } \text{Tr}(b^2) = 0, \\ p^{m-2} - p^{-2}\bar{\eta}(-1)G\bar{G}, & \text{if } \text{Tr}(b^2) \neq 0, \text{Tr}(b) \neq 0, \bar{\eta}(\text{Tr}(b^2)) = 1, \\ p^{m-2} + p^{-2}\bar{\eta}(-1)G\bar{G}, & \text{if } \text{Tr}(b^2) \neq 0, \text{Tr}(b) \neq 0, \bar{\eta}(\text{Tr}(b^2)) = -1, \\ p^{m-2} + p^{-2}\bar{\eta}(-1)(p-1)G\bar{G}, & \text{if } \text{Tr}(b^2) \neq 0, \text{Tr}(b) = 0, \bar{\eta}(\text{Tr}(b^2)) = 1, \\ p^{m-2} - p^{-2}\bar{\eta}(-1)(p-1)G\bar{G}, & \text{if } \text{Tr}(b^2) \neq 0, \text{Tr}(b) = 0, \bar{\eta}(\text{Tr}(b^2)) = -1. \end{cases}$$

In order to determine the weight distribution of \mathcal{C}_D of (1.1) in Theorem 5, we need the next two lemmas.

Lemma 22 (see [9], Lemma 9) *For each $c \in \mathbb{F}_p$, set*

$$u_c = |\{x \in F_q : \text{Tr}(x^2) = c\}|.$$

If m is odd, then

$$u_c = p^{m-1} + p^{-1}\bar{\eta}(-1)\bar{\eta}(c)G\bar{G}.$$

Lemma 23 *Let m be odd with $p \mid m$. For each $c \in \mathbb{F}_p^*$, set*

$$v_c = |\{x \in F_q : \text{Tr}(x^2) = c, \text{Tr}(x) = 0\}|.$$

Then

$$v_c = p^{m-2} + p^{-1}\bar{\eta}(-1)\bar{\eta}(c)G\bar{G}.$$

Proof The proof of this lemma is similar to that of Lemma 16 and we omit the details.

Now we are ready to prove Theorem 5. Note that $2 \nmid m$ and $p \mid m$. By Lemma 14, we have $n_0 = p^{m-1}$. It follows from (3.1) and Lemma 21 that $\text{wt}(c_b) = n_0 - |N_b|$

$$\in \left\{ (p-1)p^{m-2}, (p-1)p^{m-2} \pm \frac{1}{p^2}\bar{\eta}(-1)G\bar{G}, (p-1)p^{m-2} \pm \frac{1}{p^2}\bar{\eta}(-1)(p-1)G\bar{G} \right\}.$$

Suppose

$$\begin{aligned} \omega_1 &= (p-1)p^{m-2}, \\ \omega_2 &= (p-1)p^{m-2} + \frac{1}{p^2}\bar{\eta}(-1)G\bar{G}, \\ \omega_3 &= (p-1)p^{m-2} - \frac{1}{p^2}\bar{\eta}(-1)G\bar{G}, \\ \omega_4 &= (p-1)p^{m-2} - \frac{1}{p^2}\bar{\eta}(-1)(p-1)G\bar{G}, \\ \omega_5 &= (p-1)p^{m-2} + \frac{1}{p^2}\bar{\eta}(-1)(p-1)G\bar{G}. \end{aligned}$$

By Lemmas 21, 22 and 23, we have $A_{\omega_1} = p^{m-1} - 1$ and the following system of equations:

$$\begin{cases} A_{w_2} + A_{w_4} = \frac{1}{2}(p-1)(p^{m-1} + p^{-1}\bar{\eta}(-1)G\bar{G}), \\ A_{w_3} + A_{w_5} = \frac{1}{2}(p-1)(p^{m-1} - p^{-1}\bar{\eta}(-1)G\bar{G}), \\ A_{w_4} = \frac{1}{2}(p-1)(p^{m-2} + p^{-1}\bar{\eta}(-1)G\bar{G}), \\ A_{w_5} = \frac{1}{2}(p-1)(p^{m-2} - p^{-1}\bar{\eta}(-1)G\bar{G}). \end{cases} \quad (3.4)$$

Solving the system of equations of (3.4) proves the weight distribution of Table 3.

3.4 The second case of five-weight linear codes

In this subsection, put $2 \nmid m$ and $p \nmid m$. The last auxiliary result we need is the following.

Lemma 24 *Let $b \in \mathbb{F}_q^*$ and the symbols be the same as before. Then*

$$|N_b| = \begin{cases} p^{m-2}, & \text{if } \text{Tr}(b^2) = 0 \text{ and } \text{Tr}(b) \neq 0, \\ p^{m-2} + p^{-1}\bar{\eta}(-m)G\bar{G}, & \text{if } \text{Tr}(b^2) = 0 \text{ and } \text{Tr}(b) = 0 \\ p^{m-2} - p^{-2}\bar{\eta}(-\text{Tr}(b^2))G\bar{G}, & \text{if } \text{Tr}(b^2) \neq 0, \text{Tr}(b) \neq 0 \text{ and } (\text{Tr}(b))^2 \neq m\text{Tr}(b^2) \\ & \text{or } \text{Tr}(b^2) \neq 0 \text{ and } \text{Tr}(b) = 0, \\ p^{m-2} + p^{-2}\bar{\eta}(-m)(p-1)G\bar{G}, & \text{if } \text{Tr}(b^2) \neq 0, \text{Tr}(b) \neq 0 \text{ and } (\text{Tr}(b))^2 = m\text{Tr}(b^2). \end{cases}$$

Proof This lemma follows from (3.2), Lemmas 14 and Lemma 15,

With the help of preceding lemmas we can now prove Theorem 8. If $2 \nmid m$ and $p \nmid m$, by Lemma 14, we have

$$n_0 = p^{m-1} + p^{-1}\bar{\eta}(-m)G\bar{G}.$$

By Lemma 24, we know $wt(c_b)$ has five possible values. Let

$$\begin{aligned} w_1 &= (p-1)p^{m-2} + \frac{1}{p}\bar{\eta}(-m)G\bar{G}, & w_2 &= (p-1)p^{m-2}, \\ w_3 &= (p-1)p^{m-2} + \frac{1}{p^2}(p\bar{\eta}(-m) + 1)G\bar{G}, \\ w_4 &= (p-1)p^{m-2} + \frac{1}{p^2}(p\bar{\eta}(-m) - 1)G\bar{G}, \\ w_5 &= (p-1)p^{m-2} + p^{-2}\bar{\eta}(-m)G\bar{G}. \end{aligned}$$

It follows from Lemmas 17, 18 and 24 that

$$\begin{aligned} A_{\omega_1} &= (p-1)(p^{m-2} - p^{-2}\bar{\eta}(-m)G\bar{G}), \\ A_{\omega_2} &= p^{m-2} + p^{-2}\bar{\eta}(-m)(p-1)G\bar{G} - 1, \\ A_{\omega_5} &= (p-1)p^{m-2} + p^{-2}\bar{\eta}(-m)(p-1)^2G\bar{G}, \end{aligned}$$

where A_{w_i} denotes the frequency of w_i . It can be easily checked that the minimum distance of the dual code \mathcal{C}_D^\perp of \mathcal{C}_D is equal to 2. By the first two Pless Power Moments ([12], p. 260) the frequency A_{w_i} of w_i satisfies the following equations:

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} + A_{w_4} + A_{w_5} = p^m - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_3} + w_4 A_{w_4} + w_5 A_{w_5} = p^{m-1}(p-1)n, \end{cases} \quad (3.5)$$

where $n = p^{m-1} + p^{-1}\overline{\eta}(-m)G\overline{G} - 1$. A simple manipulation leads to the weight distribution of Table 4.

4 Concluding Remarks

In this paper, we present a class of three-weight and five-weight linear codes. There is a survey on three-weight codes in [6]. A number of three-weight and five-weight codes were discussed in [2, 3, 8, 9, 10, 17, 19, 20, 21].

Let w_{\min} and w_{\max} denote the minimum and maximum nonzero weight of a linear code \mathcal{C} . The linear code \mathcal{C} with $w_{\min}/w_{\max} > (p-1)/p$ can be used to construct a secret sharing scheme with interesting access structures (see [18]).

Let $m \geq 4$. Then for the linear code \mathcal{C}_D of Theorem 1, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{(p-1)p^{m-2} - (p-2)p^{\frac{m-2}{2}}}{(p-1)p^{m-2}} \text{ or } \frac{(p-1)p^{m-2}}{(p-1)p^{m-2} + (p-2)p^{\frac{m-2}{2}}}.$$

It can be easily checked that

$$\frac{(p-1)p^{m-2}}{(p-1)p^{m-2} + (p-2)p^{\frac{m-2}{2}}} > \frac{(p-1)p^{m-2} - (p-2)p^{\frac{m-2}{2}}}{(p-1)p^{m-2}} > \frac{p-1}{p}.$$

Hence,

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}.$$

Let $m \geq 6$. Then for the linear code \mathcal{C}_D of Theorem 3, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{(p-1)p^{m-2} - 2p^{\frac{m-2}{2}}}{(p-1)p^{m-2}} \text{ or } \frac{(p-1)p^{m-2}}{(p-1)p^{m-2} + 2p^{\frac{m-2}{2}}}.$$

Simple computation shows that

$$\frac{(p-1)p^{m-2}}{(p-1)p^{m-2} + 2p^{\frac{m-2}{2}}} > \frac{(p-1)p^{m-2} - 2p^{\frac{m-2}{2}}}{(p-1)p^{m-2}} > \frac{p-1}{p}.$$

Therefore,

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}.$$

Let $m \geq 5$. Then for the linear code \mathcal{C}_D of Theorem 5, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{(p-1)p^{m-2} - (p-1)p^{\frac{m-3}{2}}}{(p-1)p^{m-2} + (p-1)p^{\frac{m-3}{2}}} > \frac{p-1}{p}.$$

Let $m \geq 5$. Then for the linear code \mathcal{C}_D of Theorem 8, we have

$$\frac{w_{\min}}{w_{\max}} = \frac{(p-1)p^{m-2} - (p+1)p^{\frac{m-3}{2}}}{(p-1)p^{m-2}} \text{ or } \frac{(p-1)p^{m-2}}{(p-1)p^{m-2} + (p+1)p^{\frac{m-3}{2}}}.$$

It is easy to show that

$$\frac{(p-1)p^{m-2}}{(p-1)p^{m-2} + (p+1)p^{\frac{m-3}{2}}} > \frac{(p-1)p^{m-2} - (p+1)p^{\frac{m-3}{2}}}{(p-1)p^{m-2}} > \frac{p-1}{p}.$$

Then we get

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}.$$

To sum up, the linear codes \mathcal{C}_D with $m \geq 5$ can be employed to get secret sharing schemes.

Acknowledgements. This research is supported by a National Key Basic Research Project of China (2011CB302400), National Natural Science Foundation of China (61379139), the “Strategic Priority Research Program” of the Chinese Academy of Sciences, Grant No. XDA06010701 and Foundation of NSSFC(No.13CTJ006).

References

1. S.-T. Choi, J.-Y. Kim, J.-S. No, and H. Chung, “Weight distribution of some cyclic codes,” in Proc. Int. Symp. Inf. Theory, pp. 2911–2913, 2012.
2. B. Courteau, J. Wolfmann, “On triple-sum-sets and two or three weights codes,” *Discrete Mathematics*, vol. 50, pp.179-191, 1984.
3. C. Ding, “A class of three-weight and four-weight codes,” in: C. Xing, et al. (Eds.), Proc. of the Second International Workshop on Coding Theory and Cryptography, in: Lecture Notes in Computer Science, vol. 5557, Springer Verlag, pp. 34-42, 2009.
4. C. Ding, “Linear codes from some 2-designs,” *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3265-3275, 2015.
5. C. Ding, J. Luo, H. Niederreiter, “Two-weight codes punctured from irreducible cyclic codes,” in: Y. Li, et al. (Eds.), Proceedings of the First Workshop on Coding and Cryptography, World Scientific, Singapore, pp. 119-124, 2008.
6. C. Ding, C. Li, N. Li, and Z. Zhou, “Three-weight cyclic codes and their weight distributions,” submitted for publication.
7. C. Ding, J. Yang, “Hamming weights in irreducible cyclic codes,” *Discrete Math.*, vol. 313, no. 4, pp. 434–446, 2013.
8. C. Ding, Y. Gao, Z. Zhou, “Five Families of Three-Weight Ternary Cyclic Codes and Their Duals,” *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7940–7946, 2013.
9. K. Ding, C. Ding, “Bianry linear codes with three weights,” *IEEE Communication Letters*, vol. 18, no. 11, pp. 1879–1882, 2014.
10. K. Ding, C. Ding, “A class of two-weight and three-weight codes and their applications in secret sharing,” arxiv:1503.06512v1.

11. M. Grassl, Bounds on the minimum distance of linear codes, available online at <http://www.codetables.de>.
12. W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge: Cambridge University Press, 2003.
13. C. Li, Q. Yue, and F. Li, Hamming weights of the duals of cyclic codes with two zeros, *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 3895–3902, Jul. 2014.
14. C. Li, Q. Yue, and F. W. Fu, “Complete weight enumerators of some cyclic codes,” *Des. Codes Cryptogr.*, DOI 10.1007/s10623-015-0091-5, 2015.
15. R. Lidl, H. Niederreiter, *Finite fields*. Cambridge University Press, New York (1997)
16. Q. Wang, K. Ding, R. Xue, “Binary linear codes with two weights” *IEEE Communication Letters*, vol. 19, no. 7, Jul. 2015.
17. C. Xiang, “A family of three-weight binary linear codes,” arxiv: 1505.07726
18. J. Yuan and C. Ding, “Secret sharing schemes from three classes of linear codes,” *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 206–212, 2006.
19. Z. Zhou, C. Ding, “A class of three-weight cyclic codes,” *Finite Fields and Their Applications*, vol. 25, pp. 79–93, 2014.
20. Z. Zhou, N. Li, C. Fan, T. Helleseeth, “Linear codes with two or three weights from quadratic bent functions,” arxiv: 1505.06830
21. Z. Zhou, C. Ding, J. Luo, A. Zhang, “A family of five-weight cyclic codes and their weight enumerators,” *IEEE Trans Inf. Theory*, vol. 59, no. 10, pp. 6674–6682, 2013.
22. Z. Zhou, A. Zhang, C. Ding, M. Xiong, “The weight enumerator of three families of cyclic codes,” *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 6002–6009, 2013.